Comments of Consumer Reports
In Response to the
California Privacy Protection Agency's
Invitation for Preliminary Comments on
Notices & Disclosures and Employee Data

By

Matt Schwartz, Senior Policy Analyst, Consumer Reports
Justin Brookman, Director of Technology Policy, Consumer Reports

May 20, 2026

Consumer Reports[1] thanks the California Privacy Protection Agency (CalPrivacy) for the opportunity to provide feedback on its Invitation for Preliminary Comments on Notices & Disclosures and Employee Data. We appreciate the spirit of this rulemaking, though we think it is worth considering whether privacy policies can or should play a central role in the consumer experience of privacy laws. We've long argued that instead of doubling-down on the failed notice-and-choice regime, privacy laws should move toward more substantive default protections, such as data minimization, that alleviate the burden on consumers to manage privacy choices in an untenably complex ecosystem.[2]

That said, we understand that CalPrivacy must operate under the constraints of the statute—and that the ancillary benefits of privacy notices that may accrue to other stakeholders, such as regulators, journalists, and advocates, justify further attention. We therefore offer several suggestions for how CCPA's rules around disclosures and notices can be improved, some of which were shared in a previous comment.[3]

Our recommendations include:

- Requiring businesses to plainly state whether they believe themselves to be covered by CCPA;
- Requiring businesses to share the precise list of third parties with whom they have sold or shared consumers' personal information;
- Requiring businesses to detail their process for verifying consumer requests;
- Strengthening enforcement against businesses with broken privacy request links.

Please note that CR does not take a position on the employer-facing aspects of this comment proceeding.

---

[1] Consumer Reports is an independent, nonprofit membership organization that works side by side with consumers to create a fairer, safer, and healthier world. For over 80 years, CR has provided evidence-based product testing and ratings, rigorous research, hard-hitting investigative journalism, public education, and steadfast policy action on behalf of consumers' interests, including their interest in securing effective privacy protections. Unconstrained by advertising, CR has exposed landmark public health and safety issues and strives to be a catalyst for pro-consumer changes in the marketplace. From championing responsible auto safety standards, to winning food and water protections, to enhancing healthcare quality, to fighting back against predatory lenders in the financial markets, Consumer Reports has always been on the front lines, raising the voices of consumers.

[2] Consumer Reports and EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking, (January 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf

[3] Matt Schwartz and Justin Brookman, Comments of Consumer Reports In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals, (April 6, 2026), https://advocacy.consumerreports.org/wp-content/uploads/2026/04/CR-Comments-CalPrivacy-Friction-and-OOPSs.pdf

General Views

Before describing how we believe that CCPA's existing notice requirements could be improved, it is worth taking stock of the role of notices in privacy laws and assessing who the audience for any such improvements should be. On the positive side of the ledger, there is some evidence that privacy policies and other consumer-facing notices and disclosure can play an important role for expert audiences and those with a particular interest in holding companies accountable for promises made to consumers—such as regulators, journalists, and advocates. As enforcers have noted, privacy policies are often a leading indicator of deeper data governance issues within a business.[4] If a business cannot clear the low bar of writing a legible or legally compliant privacy policy, it may suggest that privacy is not a priority for the business. Conversely, the very act of writing privacy policies can sometimes improve business' own understanding of their internal procedures and external relationships in a way that can improve privacy outcomes for consumers.[5]

More thorough inspection of privacy policies can also sometimes reveal prima facie privacy issues. For example, Consumer Reports' investigation of several major exercise equipment companies found that it was common for companies to give themselves permission to share health-related information with marketing and social media companies.[6] And an earlier Consumer Reports investigation into seven of the leading mental health apps showed that they had significant privacy issues: many shared user and device information with social media companies and all had confusing privacy policies that few consumers would understand.[7]

However, there is substantially less evidence that privacy notices currently serve an systemically important role for consumers themselves—or that tinkering with the form of privacy notices can make a tangible improvement to consumers' understanding of inherently complex company data processing activities. The vast majority of consumers do not read privacy policies,[8] and if even they did, it would likely not be a productive use of time. More than 15 years ago, researchers from Carnegie Mellon University estimated that the average internet user encounters an average of 1,462 privacy policies a year, and that it would take a user an average of 244 hours

---

[4] Josh Hansen, From Policies to Practice: What Regulators Expect from Privacy Programs, (April 14, 2026), https://www.jdsupra.com/legalnews/from-policies-to-practice-what-2886801/

[5] Peter Swire, The Surprising Virtues of the New Financial Privacy Law, 86 MINN. L. REV. 1263, 1316 (2002), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=3082&context=mlr

[6] Catherine Roberts, Your Exercise Bike Knows a Lot About You—and It Doesn't Keep Every Secret, Consumer Reports, (January 14, 2025), https://www.consumerreports.org/health/health-privacy/exercise-machine-privacy-a3907557984/

[7] Thomas Germain, Mental Health Apps Aren't All As Private As You May Think, Consumer Reports, (March 2, 2021), https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/

[8] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information 5 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf

per year to read the privacy policy of every website they visited.[9] The number, length, and complexity of privacy policies have surely only skyrocketed since then and Carnegie Mellon's estimate does not account for the time it would take for consumers to *comprehend* the privacy notices, only to read them.

The obvious pushback is that privacy policies should therefore be made simpler and more legible for the average consumer. But as privacy scholar Helen Nissenbaum has pointed out, there is an inherent "transparency paradox" whereby the more readable and simpler privacy policies are, the less meaningful and accurate they are likely to be.[10] Simplified privacy "nutrition labels" appear to modestly improve consumer understanding,[11] but risk obfuscating more complex risks associated with data collection or transfer and are often inaccurate in practice.[12] This is likely to become an even greater issue as company data processing activities increase in complexity or further rely on "black box" algorithms that the companies cannot even themselves fully explain.

It is also worth mentioning at the outset that CCPA and the regulations already include fairly detailed requirements for the content and form of privacy notices. Privacy notices and disclosures are required to use "straightforward language and avoid technical or legal jargon"[13], to offer a "comprehensive description of the business' online and offline information practices,"[14] and to clearly disclose how certain categories of personal information are collected and with whom they are shared.[15] Anecdotally, it appears that many businesses are not complying with these baseline requirements, especially those around readability (subjective as the standards may be). In practice, more vigorous enforcement of existing privacy policy requirements may go further than additional requirements, especially if those additional requirements are not backed up with additional enforcement resources.

These concerns around the efficacy of privacy policies are part of the reason why CR supports the concept of data minimization—the idea that privacy laws should restrict businesses to only collect and use personal information that is necessary to provide the service requested by consumers. By putting the onus of protection on businesses, consumers are spared from making endless consent choices or having to read company privacy policies.

---

[9] Aleecia M. McDonald and Lorrie Faith Cranor, I/S: A Journal of Law and Policy for the Information Society, The Cost of Reading Privacy Policies, (2008), https://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[10] Helen Nissenbaum, the Journal of the American Academy of Arts & Sciences, A Contextual Approach to Privacy Online, (2011), https://nissenbaum.tech.cornell.edu/papers/Contextual%20Approach%20to%20Privacy%20Online.pdf

[11] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, Robert W. Reeder, Carnegie Mellon University, A "Nutrition Label" for Privacy, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

[12] Mozilla Study: Data Privacy Labels for Most Top Apps in Google Play Store are False or Misleading, February 23, 2023, https://www.mozillafoundation.org/en/privacynotincluded/articles/mozilla-study-data-privacy-labels-for-most-top-apps-in-google-play-store-are-false-or-misleading/#:~:text=The%20study%20%E2%80%93%20%E2%80%9CSee%20No%20Evil,provide%20false%20or%20misleading%20information.

[13] CCPA Rules Section 7003(a)

[14] Id., Section 7011(e)(1)

[15] Id.

That said, while we continue to believe that strengthening the data minimization provisions in privacy laws is the best way to improve privacy outcomes for consumers, we do have some suggestions for how CCPA's notice and disclosure requirements could be improved.

Responses to Select CalPrivacy Questions

When reviewing a privacy policy or similar disclosure, what is the most important information to consumers? What information about a business's collection, use, disclosure, and retention of personal information do consumers want but currently cannot find in existing privacy policies or similar disclosures?

While businesses are already required to disclose some of the most relevant information to consumers about business' collection, use, disclosure, and retention of personal information, we believe additional requirements may help consumers better understand their rights.

We offer the following recommendations.

Businesses Should Have to Plainly State if They Are Covered by CCPA

As described in a previous comment,[16] we believe that businesses should be required to plainly state if they believe themselves to be covered by CCPA. It should be simple for consumers to understand whether the company they are interacting with constitutes a "covered entity" under the CCPA and thus is legally required to honor their rights requests. Unfortunately, companies do not always offer clear indications of whether they meet the legal thresholds defined in CCPA Section 1798.140(d) (e.g., the $25 million revenue threshold or the 100,000 consumer data processing trigger) and consumers lack any ability to independently verify these figures.

Many companies' privacy notices are vague about their compliance status per jurisdiction, only offering that consumer rights "may" apply depending on the location of the requester, such as in the following example:

> The additional disclosures that we provide in this Notice are required in a growing number of jurisdictions ("Data Privacy Laws"), and we believe are simply good business practice. Depending on where you live and subject to certain exceptions, you may have some or all of the following rights:

The uncertainty that such disclosures engender may result in a form of informational friction that discourages consumers from even attempting to exercise their rights in the absence of clear evidence that such efforts will be worthwhile. And while the presence of certain design features

[16] Matt Schwartz and Justin Brookman, Comments of Consumer Reports In Response to the California Privacy Protection Agency's Invitation for Preliminary Comments on Reducing Friction in the Exercise of Privacy Rights and Opt-Out Preference Signals, (April 6, 2026), https://advocacy.consumerreports.org/wp-content/uploads/2026/04/CR-Comments-CalPrivacy-Friction-and-OOPSs.pdf

(e.g. the existence of a “Do Not Sell My Personal Information” footer) or privacy policy verbiage (e.g. a California-specific section of the privacy policy) imply that a company is required to comply with CCPA, these are imperfect indicators and in any case are likely only to be interpreted as such by the most sophisticated consumers.

We therefore recommend a plain disclosure of compliance status along the following lines:

> *“The description of consumer rights must unambiguously indicate those rights are available to California residents. Statements such as “you may have rights” or “if your state has a data privacy law” are not sufficiently clear to inform California residents of their rights. Businesses must state the described consumer rights may be exercised by either (i) all users or all United States users or (ii) clearly describe the subset of users, including explicitly identifying California residents, among residents of other states.”*[17]

Businesses Should Disclose List of Third Parties to Whom they have Sold or Shared Personal Information

One of the privacy policy-related areas we’ve seen states improve on the CCPA is by requiring covered businesses to disclose the precise list of third-parties to which the business has sold or shared the consumers information (rather than just the categories of third-parties). Other states require businesses to either disclose this information in a section of the privacy policy itself,[18] or to do so upon the request of the consumer.[19] Businesses typically have the choice of either disclosing the list of third-parties that they have sold or shared a particular consumer’s data to, or disclosing the list of *all* third-parties to which they have sold or shared personal information.

In some cases, a list of data recipients is likely to be highly material to a consumer’s consent choice. For example, if a health website shares personal data with social media companies, a consumer may think twice about providing especially sensitive information. In addition, such disclosures are very helpful for enforcers and advocates to trace the flow of personal information and to hold companies accountable for their promises.

A third-party disclosure requirement could be created via rulemaking under the authority granted to CalPrivacy through Section 1798.185(a)(6), which allows the Agency to create rules and procedures to “facilitate” a consumer’s ability to obtain information pursuant to Section 1798.130.

---

[17] This formulation is derived from the Delaware AG’s Delaware Privacy Act FAQs, https://attorneygeneral.delaware.gov/fraud/personal-data-privacy-portal/frequently-asked-questions/

[18] Rhode Island General Laws. § 6-48.1-3(a)(2), "Information Sharing Practices", https://webserver.rilegislature.gov/Statutes/TITLE6/6-48.1/6-48.1-3.htm.

[19] Minnesota Statutes, 325M.14(Sub. 1(a)(h)), https://www.revisor.mn.gov/statutes/cite/325M/full; Oregon SB 619, Section 3(1)(a)(B), https://olis.oregonlegislature.gov/liz/2023R1/Downloads/MeasureDocument/SB619/Enrolled

Businesses Should Be Required to Disclose Verification Procedures

Another point of friction for consumers is the back-and-forth that often ensues when businesses do not disclose in their privacy documentation all of the necessary information needed from consumers in order to make a successful request. For example, consumers may submit requests to access, correct, or delete through email or the webform only to find out days or weeks later that they must in fact log-in to their existing account to complete the request (as provided for under Section 7061(a) of the Rules). Additionally, some businesses have complained about consumers submitting *too much* personal information in emailed rights requests, despite not clearly delineating in their privacy policy the minimum information necessary to successfully action a request. Businesses should be required to disclose the required verification steps to consumers either in the privacy policy, or, ideally, at the point of the privacy request itself so that consumers do not waste time by submitting insufficiently detailed requests. And if the business accepts requests via a mechanism that does not automatically delineate the necessary submission fields (e.g. email, or toll-free phone number), it should also be required to disclose the minimum information necessary to action a request in their privacy policy.

Expectations for Addressing Broken Links Should Be Higher

Another key source of friction is the presence of broken links within company privacy policies, request forms, or other key privacy documentation. Obviously, without access to these resources, consumers cannot complete requests and are more likely to simply give up than to attempt to redress these issues with companies. Section 7004(a)(5)(B) already states that "a business that knows of, but does not remedy, circular or broken links…may be in violation of this regulation," but clearly this warning has not been heeded as well as it should be. CalPrivacy should strengthen this provision to state that businesses that don't fix broken links within a reasonable time-frame *are* in violation of the law and should monitor compliance with this provision as an element of any future enforcement sweeps.

What language in privacy policies do consumers find confusing, unclear, or difficult to understand? How can CalPrivacy address this issue?

One possibility would be to require businesses to share the subset of key information about their practices required in the Notice at Collection at the very top of a privacy policy. This would prevent consumers from having to hunt down the most relevant information, which may be hiding in far-flung regions of the privacy policy and may better facilitate their ability to make decisions.

A list of key information for the short-form notice may include:

- Whether the business is covered by CCPA.

- Whether or not the business is selling or sharing personal information to third-parties and for what purposes.
- Whether or not the business is selling or sharing sensitive information.
- A brief description of the categories of personal information being collected.
- A direct link to make a rights request.

What are effective ways for consumers to receive notice of their CCPA rights and how to exercise those rights? For example, how do effective notice mechanisms differ across mobile apps, internet connected devices, smartwatches, smart TVs, home appliances, gaming systems, or other interfaces that do not support traditional webpage-based notices?

Please provide examples of effective consumer notices and disclosures. If possible, please provide information about specific testing, studies, or data demonstrating their effectiveness.

While CR does not maintain a list of effective consumer notices and disclosures, we have encountered a variety of *ineffective* disclosures.

Some key examples:

- Consent flows that are presented to consumers in high-stress situations or part of a larger onboarding processes, such as when consumers purchase a car through a dealership, can lead to major gaps in consumer understanding. For example, the New York Times reported how the consent screens shown to millions of GM car purchasers were deceptive and led to consumers unknowingly consenting to having their personal information shared for insurance pricing purposes.[20]
- Modern smart televisions often collect invasive information from consumers under the guise of "automatic content recognition" are similarly euphemistic terminology. These settings are often difficult to identify and require multi-step processes to turn-off.[21] The Texas Attorney General recently sued several major TV manufacturers for alleged deficiencies in those companies' privacy policies and consent flows.[22]
- Recent research has demonstrated significant issues with the privacy disclosures of smart home devices.[23] In 14 percent of cases, researchers needed to use a smart device's companion app to review the privacy policy; in 49 percent of cases, researchers stated that the privacy policy was "difficult to obtain" (in one particularly perverse example, researchers were required to submit personal information to even access the

[20] Kashmir Hill, the New York Times, How GM Tricked Millions of Drivers into Being Spied On (Including Me), (April 25, 2024), https://www.nytimes.com/2024/04/23/technology/general-motors-spying-driver-data-consent.html
[21] James Wilcox, Consumer Reports, How to Turn Off Smart TV Snooping Features, (October 19, 2025), https://www.consumerreports.org/electronics/privacy/how-to-turn-off-smart-tv-snooping-features-a4840102036/
[22] Office of the Texas Attorney General, Attorney General Paxton Sues Five Major TV Companies, Including Some with Ties to the CCP, for Spying on Texans, (December 15, 2025),
[23] Sunil Manandhar, Kaushal Kafle, Benjamin Andow,, Kapil Singh, Adwait Nadkarni, USENIX 2022 Proceedings, Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage, https://www.adwaitnadkarni.com/downloads/manandhar-sec22.pdf

privacy policy); and in 10% of cases, the manufacturer simply did not supply a privacy policy. This is especially concerning given the scale and invasive nature of data collection often implicated in this product category.[24]

****

Thank you very much again for the opportunity to provide feedback on this important proceeding — we look forward to continuing to engage with CalPrivacy as it moves forward. We are happy to answer any questions you may have, and to discuss these issues in more detail. Please contact Justin Brookman (justin.brookman@consumer.org) or Matt Schwartz (matt.schwartz@consumer.org) for more information.

[24] Daniel Wroclawski, Consumer Reports, Smart Appliances Promise Convenience and Innovation. But Is Your Privacy Worth the Price?, (July 24, 2023), https://www.consumerreports.org/electronics/privacy/smart-appliances-and-privacy-a1186358482/